Risks and Rewards of the Internet of Things

Findings From ISACA's 2013 IT Risk/Reward Barometer

ISACA®

Trust in, and value from, information systems

The world is increasingly being populated by connected devices that collect and share information over the Internet. This Internet of Things offers business and consumers powerful benefits, but it also raises concerns about data privacy and security. This year's IT Risk/Reward Barometer, conducted by nonprofit global association ISACA, uncovers interesting gaps between what people believe and what they do when it comes to the Internet of Things and sharing information online in general, and it points to key steps that enterprises should take to provide sound governance and management of enterprise IT for this new era.

The Landscape Today

In today's broadly connected digital world, an increasing number of everyday objects have the ability to collect and transmit data through the use of embedded devices or sensors that connect with networks. Ranging from household appliances to sophisticated business tools, these devices collectively make up what is known as the Internet of Things. Cisco predicts that 50 billion objects will be connected to the Internet by 2020.[1]

The business applications for such devices are vast: organizations can track, measure and communicate with both their employees and their machinery. Vending machines, parking meters, street lamps, dumpsters — the status of each of these traditionally offline devices can now be monitored wirelessly and in real-time. Santander, a city in Spain, has 12,000 sensors that detect everything from air pollution to available parking spaces to dumpsters that need emptying. Fleet and warehouse managers are using here-and-now information to track supplies and adjust their order fulfillment and supply chain strategies. Employees can also become connected devices, so to speak, with some companies introducing wearable devices that collect information on workers' energy levels, office habits and productivity.

Connected devices are taking over the home as well. While personal fitness trackers and health monitors are nothing new, almost every appliance is becoming smarter. Refrigerators now let you take notes and write grocery lists on built-in touch screens, which then sync wirelessly with your phone. Coffee makers offer the ability to control the temperature and strength of your coffee without you ever leaving your bed. Connected thermostats and utility meters now contain activity sensors that adjust the power usage in a home if no one is there or if they sense patterns in your schedule. Wearable gadgets are also entering the space, with devices like Google Glass and smart watches hoping to crack the consumer code.

Santander, a city in Spain, has 12,000 sensors that detect everything from air pollution to available parking spaces to dumpsters that need emptying.

Organizations employing Internet of Things devices have the potential to reap numerous rewards: greater efficiency, lower costs, improved services, more accurate supply chain management, greater accessibility to information, increased employee productivity and increased customer satisfaction. However, the Internet of Things poses a number of risks as well. More connected devices means more entry points for potential hackers. Attacks on critical infrastructure components, espionage and theft of intellectual property are all very real threats. Data breaches resulting in corporate or personal

[1] Source: Cisco: *http://blogs.cisco.com/news/cisco-connections-counter/*

information being stolen or compromised could have widespread effects not only on business operations, but also on consumer trust and corporate reputation.

Challenges for IT Professionals

The impact of these issues and the task of managing them falls primarily on enterprise IT departments. This group faces a number of challenges regarding the secure and effective implementation of connected devices in their organizations. These challenges include:

- Identity and access management
- Ownership of technology and/or data by stakeholders outside of IT (e.g., marketing or HR)
- Requests to share data with authorized third parties (e.g., government)
- Unknown costs of handling and storing increasingly large volumes of data and maintaining network of devices
- Need for new or enhanced skill sets among staff
- Regulatory compliance

A Look at Risks and Rewards

Aside from the benefits that Internet of Things devices pose to enterprises, this evolution also brings with it governance issues that IT professionals are increasingly being tasked to address. To address these issues in a way that does not interfere with leveraging the benefits of these devices, IT professionals will need to understand employee attitudes and master the learning curve that goes with these devices. Consequently, ISACA decided to make the Internet of Things a major focus of its 2013 IT Risk/Reward Barometer.

The Barometer examines attitudes and behaviors related to the risks and rewards of key technology trends, which this year include Big Data and BYOD (Bring Your Own Device) in addition to the Internet of Things. (For more information on Big Data and BYOD, see the Resources section at the end.) The Barometer consists of two components:

- A survey of 2,013 ISACA members from 110 countries
- A survey of more than 4,000 consumers in four countries: US, Mexico, India and UK

What Consumers Think

The Belief/Behavior Gap

The survey examines attitudes and behaviors around connected devices, specifically as they pertain to privacy and security. The consumer survey findings suggest a number of gaps between beliefs and actions, as consumers worry about the safety of their data, yet often fail to take the necessary precautions to protect it.

Across all markets surveyed, the vast majority of consumers worry that their information will be stolen (US: 90%, Mexico: 91%, India: 88%, UK: 86%). But many still conduct risky behaviors, such as using the same two to three passwords across multiple accounts and websites (US: 51%, Mexico: 47%, India: 50%, UK: 50%) or writing down passwords so they can remember them (US: 40% , Mexico: 29%, India: 41%, UK 22 %).

Across all markets surveyed, the vast majority of consumers worry that their information will be stolen.

This conflict between concerns about privacy and security and the seeming desire for convenience will become important as connected devices spread further, since consumers—many of whom are also employees—will need to manage a growing universe of Internet connectivity and information sharing.

Lack of Institutional Trust

Almost every day the headlines feature a story about data breaches or unexpected uses of consumer information collected online or transmitted electronically. As a way of exploring consumer sentiment around this issue, this year's survey asked people which institution they would trust most with data about them that was collected via the Internet of Things devices: their doctor, the federal government, their employer, their utility company, their mobile phone services provider or the makers of the apps on their phone. They were also given the option of saying they trust all of those institutions equally or don't trust any of them. The results show that trust in all organizations and institutions surveyed is low. However, app makers in particular did not rate highly (US: 1%, Mexico: 6%, India: 8%, UK: 4%). Employers did not receive a strong vote of trust, either: across each of the four markets surveyed, 5-10% of consumers said that they trusted their employers most among the institutions surveyed (US: 6%, Mexico: 5%, India: 8%, UK: 10%).

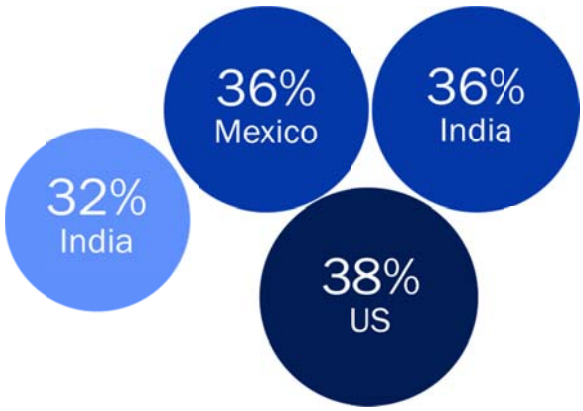
Institutional trust is a critical success factor in an increasingly connected world. If there truly will be 50 billion Internet of Things devices connected by 2020, organizations have much work to do to increase consumer (and employee) trust in how personal information is used.

Concept Is Familiar, but Name Is Not

In the US, where Internet of Things devices are readily available, fewer than one in five Americans (16%) are aware of the term "Internet of Things." Yet many have used Internet of Things devices, such as a GPS system (62%), electronic toll devices on their cars (28%) and smart TVs (20%). Millennials are the most knowledgeable about the term, as one in four (25%) had heard of it, vs. just 16% of the general population. Additionally, 32% of Millennials have used a smart TV, vs. just 20% nationally.

Across markets, time savings is seen as one of the biggest benefits of using connected devices (US: 38%, Mexico: 36%, India: 32%, UK: 36%). Meanwhile, concern that someone will hack into the device and do something malicious rates among the top concerns across markets (US: 31%, Mexico: 34%, India: 27%, UK: 24%).

TOP CONSUMER BENEFIT: TIME SAVINGS



TOP CONSUMER CONCERN: HACKERS

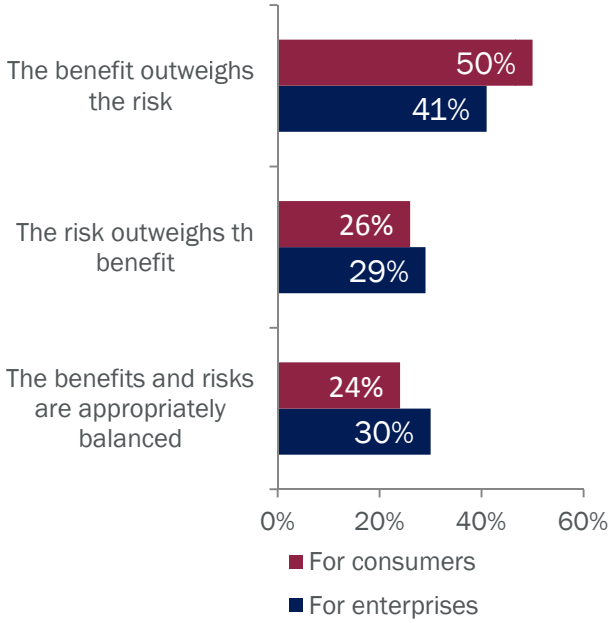
What IT Professionals Think

Benefit Outweighs Risk

On the whole, the survey found that while IT professionals acknowledge the governance issues posed by the Internet of Things, they also recognize benefits. Among IT professionals across the globe who are members of ISACA, almost all (99%) believe that the Internet of Things poses some type of governance issue, yet more than half (51%) already have plans to capitalize on the Internet of Things, and 31% say their enterprises have already benefited from greater access to information via Internet of Things devices.

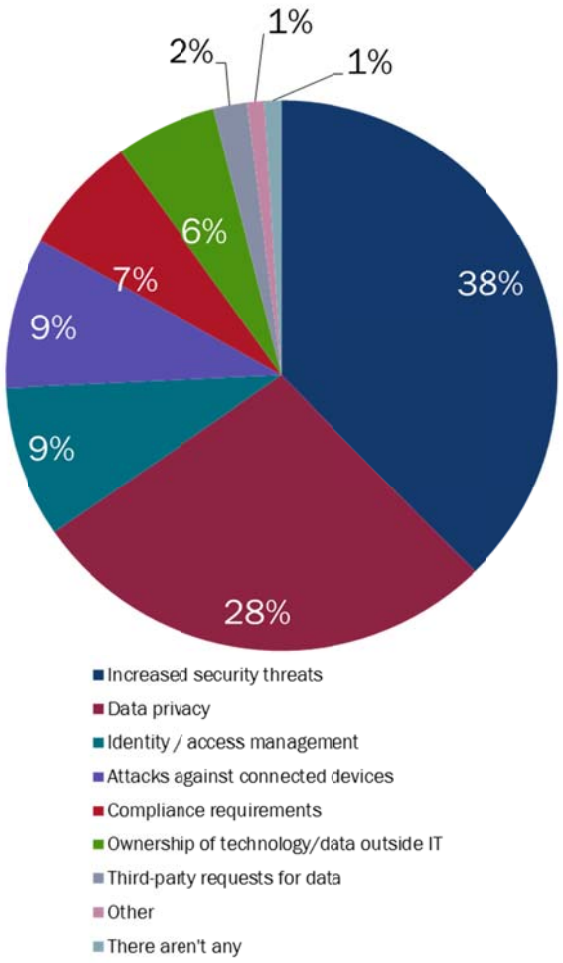
Despite perceived governances issues, half of IT professionals (50%) believe the benefit of the Internet of Things outweighs the risk for average consumers, while 41% feel that way for enterprises (vs. 29% who say the risk outweighs the benefit for enterprises).

RISK VS. BENEFIT: WHAT IT PROFESSIONALS THINK



Increased security threats are perceived as the biggest governance issue (38%), followed by data privacy at 28%.

TOP GOVERNANCE ISSUE



And although consumers are typically most concerned about people hacking into their connected devices, ISACA members believe consumers should be most concerned about not knowing who has access to their information (44%) and not knowing how their information will be used (29%).

Implications for Business and IT

Internet of Things is not just the next generation of connected devices; it involves issues such as

cybersecurity, big data and BYOD, and it raises fundamental corporate governance issues.

As this year's Risk/Reward Barometer shows, the push/pull relationship people have with technology risk and reward takes on a whole new level in the Internet of Things era. Far more personal information is shared, and it is shared in ways that the average consumer finds hard to see or control.

Five Steps to Being Agile in a Connected World

ISACA recommends that organizations adopt a five-step "Agile" process now to ensure trust and to capture value as they seek to leverage increasingly sensitive information in the Internet of Things era:

- Act quickly; enterprises cannot afford to be reactive.
- Govern the initiative to ensure that data remain secure and risks are managed.
- Identify expected benefits and how to measure them.
- Leverage internal technology steering committee to communicate benefits to the board.
- Embrace creativity and encourage innovation.

Related Resources

COBIT 5 Framework (www.isaca.org/cobit)
Privacy and Big Data (www.isaca.org/privacy-and-big-data)
Securing Mobile Devices Using COBIT 5 for Information Security (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx)
Full survey results and related infographics (www.isaca.org/risk-reward-barometer)

About the 2013 IT Risk/Reward Barometer

The annual IT Risk/Reward Barometer is a global indicator of trust in information. Conducted by ISACA, a global association of 110,000 IT security, assurance, risk and governance professionals, the Barometer polls thousands of business and IT professionals and consumers worldwide to uncover attitudes and behaviors about essential technologies and information, and the trade-offs people make to balance risk and reward. The study is based on September 2013 online polling of 2,013 ISACA members from 110 countries. Additional online surveys were fielded by M/A/R/C Research among 1,216 consumers in the US, 1,001 consumers in India, and 1,001 consumers in Mexico. The US survey ran 16–18 September 2013, and the India and Mexico surveys ran 25 September–5 October 2013. At a f90 percent confidence level, the margin of error for each individual country sample is +/- 2.8 percent. A UK survey of 1,000 employed consumers was conducted by OnePoll on 2 October 2013 with a margin of error of +/- 3.9 percentage points at the 95 percent confidence level. To see the full results, visit www.isaca.org/risk-reward-barometer.

ISACA

With 110,000 constituents in 180 countries, ISACA® (www.isaca.org) is a global association that helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. ISACA advances and validates business-critical skills and knowledge through the globally the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises govern and manage their information and technology.